Experiment 6: FTP

AIM:

Installation of Open SSH between two ubuntu machines.

DESCRIPTION:

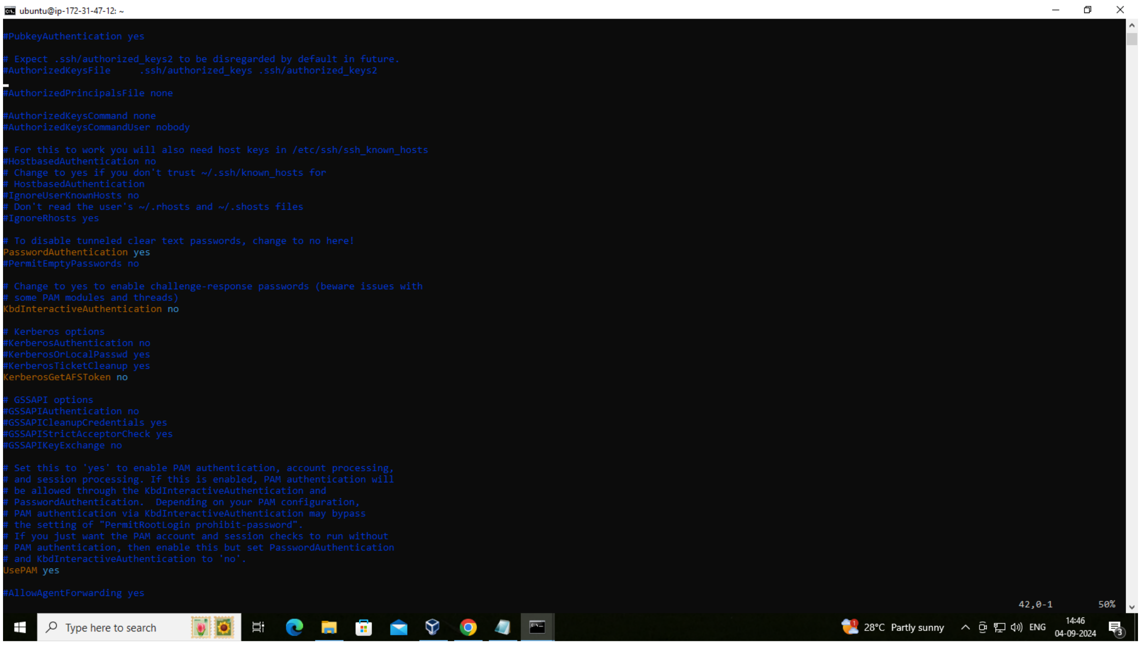
Remote File Sharing using SSH
OpenSSH is a powerful collection of tools for the remote control of, and transfer of
data between, networked computers. You will also learn about some of the configuration settings possible with the OpenSSH server application and how to change them on your Ubuntu system.
OpenSSH is a freely available version of the Secure Shell (SSH) protocol family of
tools for remotely controlling, or transferring files between computers. Traditional tools used to accomplish these functions, such as telnet or rcp, are insecure and transmit the user's password in cleartext when used. OpenSSH provides a server daemon and client tools to facilitate secure, encrypted remote control and file transfer operations, effectively replacing the legacy tools.

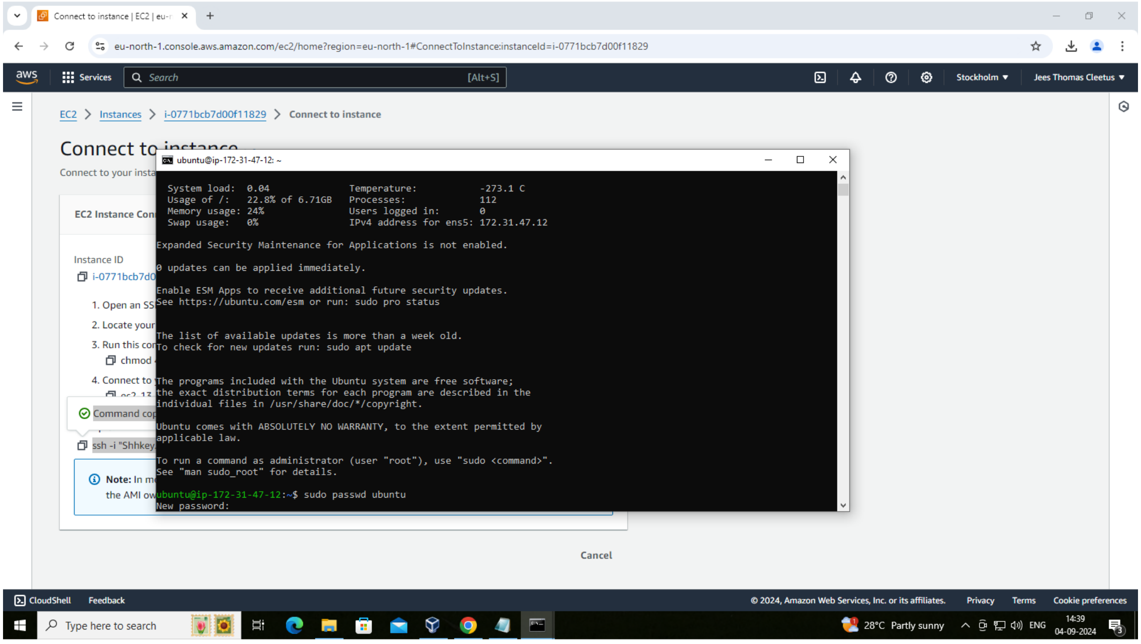
Port No: 22
Package name: openssh-client
Configuration file: /etc/ssh/sshd_config

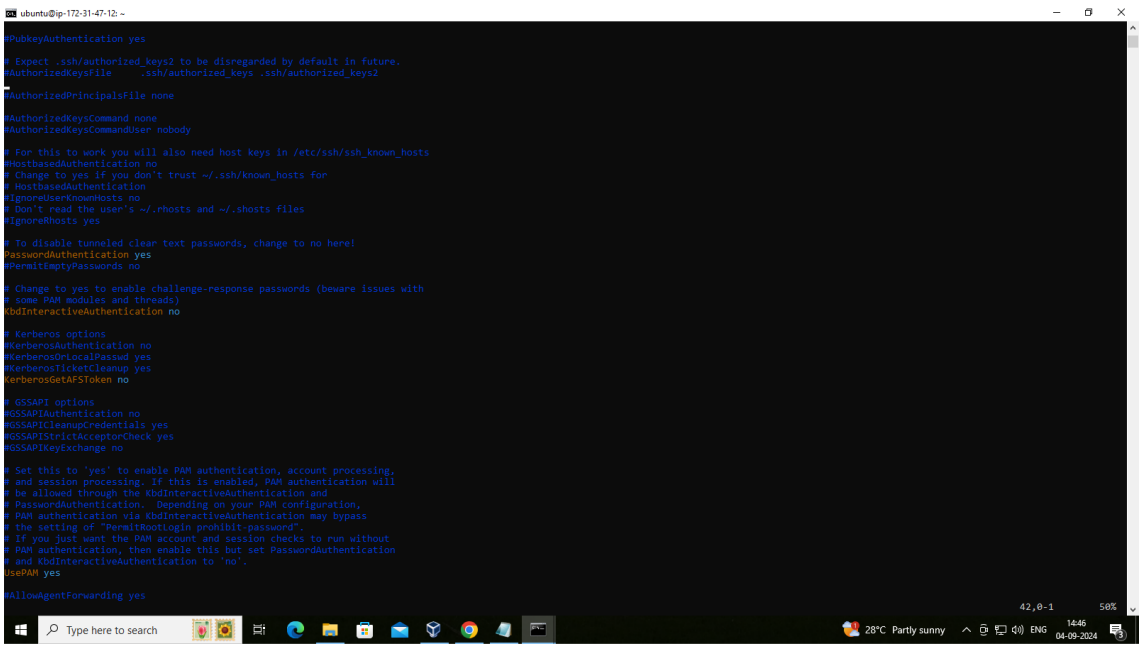
PROCEDURE:

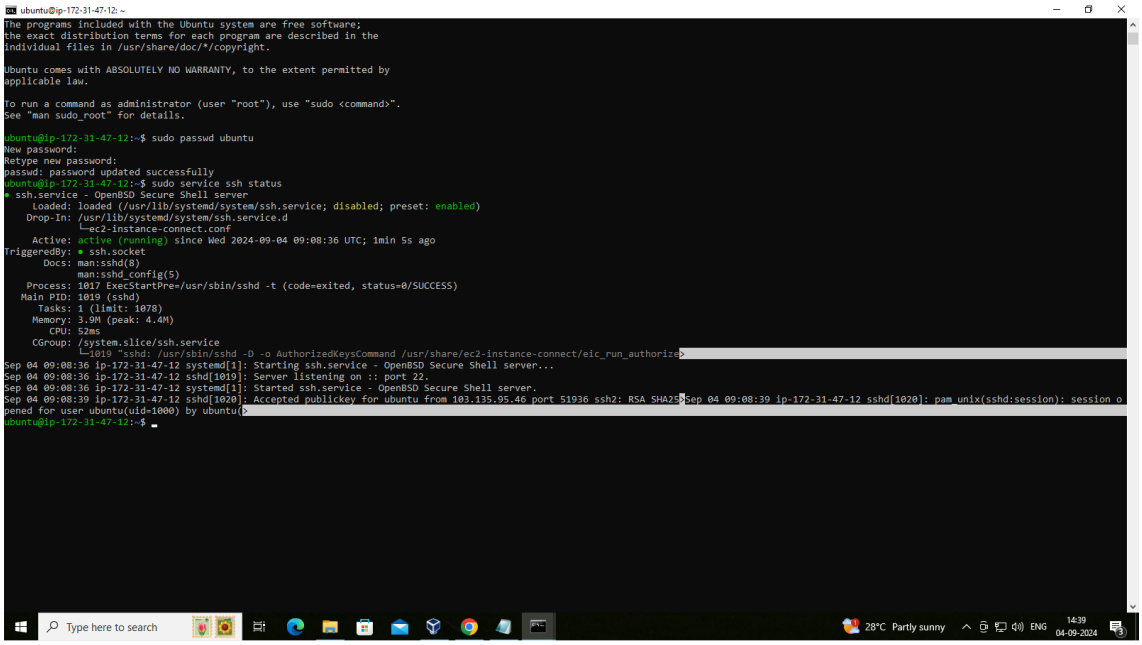
1. create two EC2 instance of ubuntu ssh client and ssh server
2. Create the password for the instance of ssh server by
   $sudo passwd ubuntu
3. Now check whether the ssh server is running by the command
   $sudo service ssh status
4. configure the sshd_config file by the following command
   $sudo vim /etc/ssh/sshd_config and include the following changes
5. PasswordAuthentication yes , KbdInteractiveAuthentication no,KerberosGetAFSToken no
6. Now check the status of the ssh server by the command
   $sudo service ssh status
7. Now create a text file by the command $touch text.txt
8. Now log in to the ssh_client and create a ssh_keygen by the command
   $ssh_keygen
9. Now copy the ssh_keygen form the ssh_client
   $ssh-copy-id ubuntu@privateip
10. Now restart the client machine
11. Then connect to the ssh_server by ssh_client, then type ls you will be prompted with the screen with your text file which you have created.

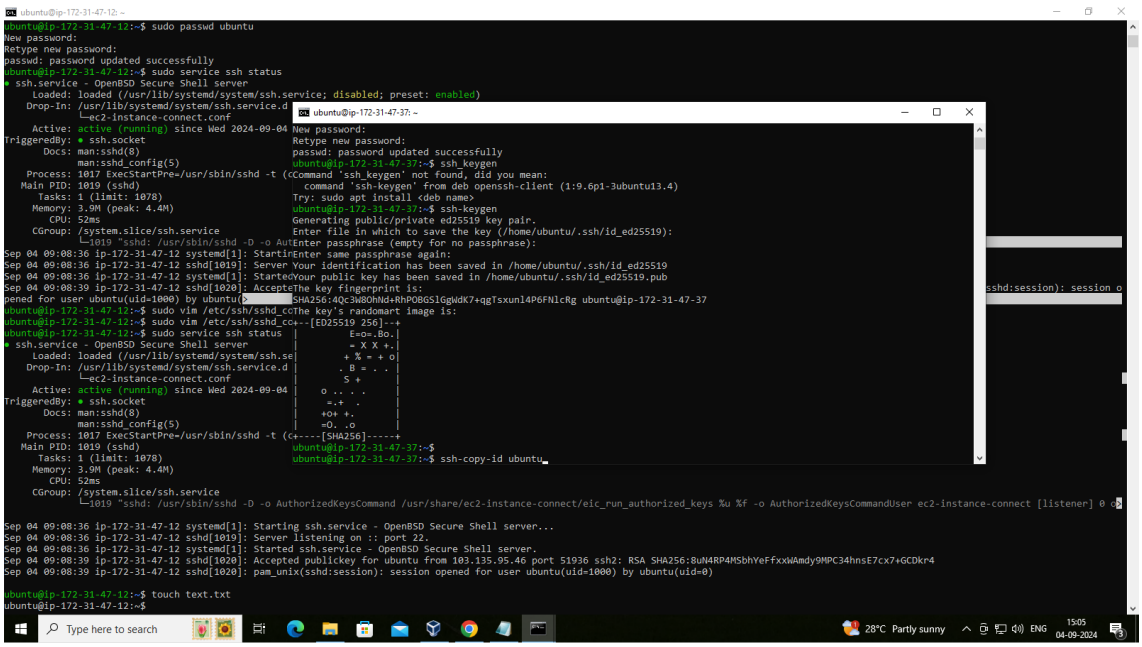
RESULT:

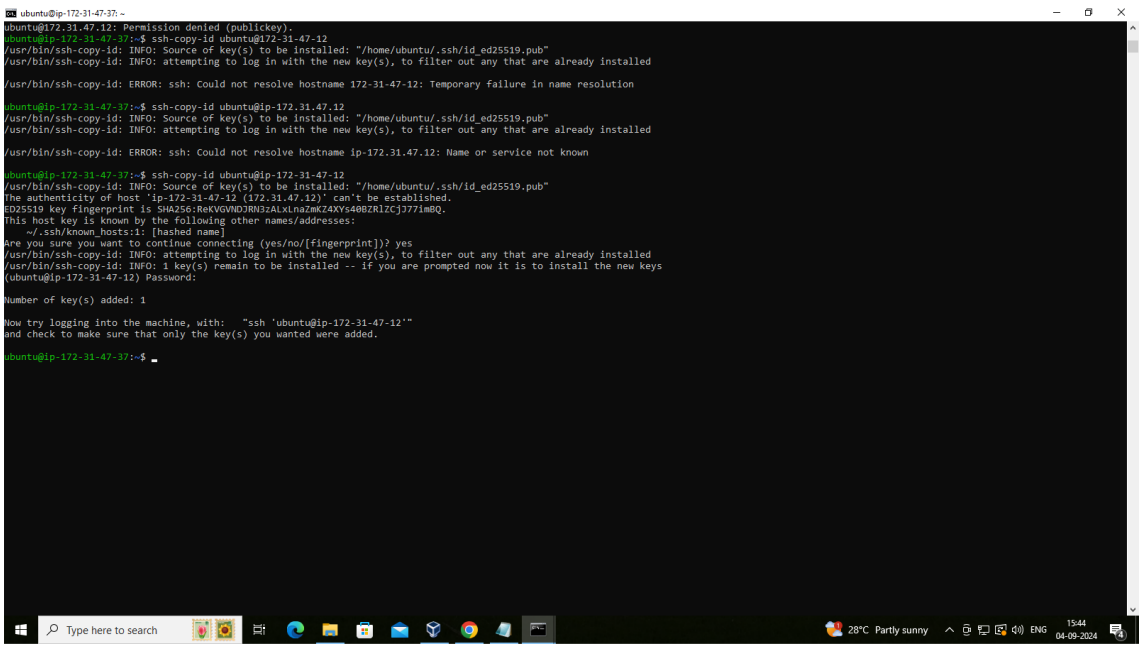

ubuntu@ip-172-31-47-12: ~
#PubkeyAuthentication yes
Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
Change to yes if you don't trust ~/.ssh/known_hosts for
HostbasedAuthentication
#IgnoreUserKnownHosts no
Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
Change to yes to enable challenge-response passwords (beware issues with
some PAM modules and threads)
KbdInteractiveAuthentication no
Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
KerberosGetAFSToken no
GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
Set this to 'yes' to enable PAM authentication, account processing,
and session processing. If this is enabled, PAM authentication will
be allowed through the KbdInteractiveAuthentication and
PasswordAuthentication. Depending on your PAM configuration,
PAM authentication via KbdInteractiveAuthentication may bypass
the setting of "PermitRootLogin prohibit-password".
If you just want the PAM account and session checks to run without
PAM authentication, then enable this but set PasswordAuthentication
and KbdInteractiveAuthentication to 'no'.
UsePAM yes
#AllowAgentForwarding yes
42,0-1 50%
Type here to search
28°C Partly sunny
ENG
14:46
04-09-2024

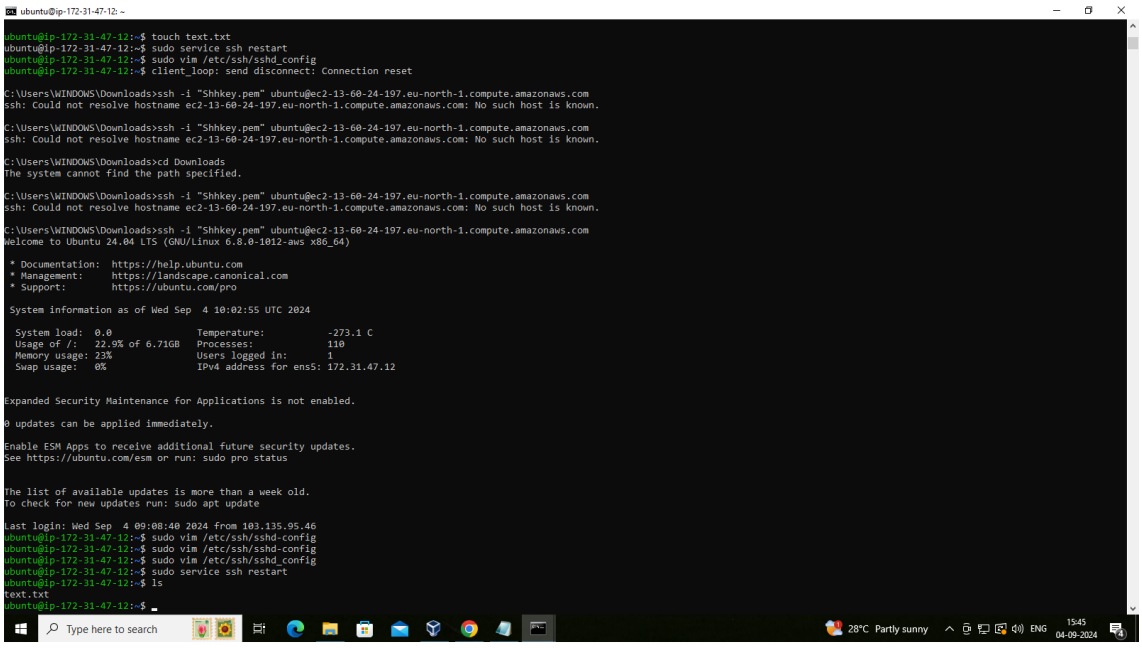

Connect to instance | EC2 | eu-n
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#ConnectToInstance:instanceId=i-0771bcb7d00f11829
Services
Search [Alt+S]
Stockholm
Jees Thomas Cleetus
EC2 > Instances > i-0771bcb7d00f11829 > Connect to instance
Connect to instance
ubuntu@ip-172-31-47-12: ~
System load: 0.04 Temperature: -273.1 C
Usage of /: 22.8% of 6.71GB Processes: 112
Memory usage: 24% Users logged in: 0
Swap usage: 0% IPv4 address for ens5: 172.31.47.12
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-47-12:~$ sudo passwd ubuntu
New password:
Cancel
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
28°C Partly sunny
ENG
14:39
04-09-2024


ubuntu@ip-172-31-47-12: ~
#PubkeyAuthentication yes
Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
Change to yes if you don't trust ~/.ssh/known_hosts for
HostbasedAuthentication
#IgnoreUserKnownHosts no
Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
Change to yes to enable challenge-response passwords (beware issues with
some PAM modules and threads)
KbdInteractiveAuthentication no
Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
KerberosGetAFSToken no
GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
Set this to 'yes' to enable PAM authentication, account processing,
and session processing. If this is enabled, PAM authentication will
be allowed through the KbdInteractiveAuthentication and
PasswordAuthentication. Depending on your PAM configuration,
PAM authentication via KbdInteractiveAuthentication may bypass
the setting of "PermitRootLogin prohibit-password".
If you just want the PAM account and session checks to run without
PAM authentication, then enable this but set PasswordAuthentication
and KbdInteractiveAuthentication to 'no'.
UsePAM yes
#AllowAgentForwarding yes
42,0-1 50%
Type here to search
28°C Partly sunny
ENG
14:46
04-09-2024


ubuntu@ip-172-31-47-12: ~
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-47-12:~$ sudo passwd ubuntu
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-47-12:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Drop-In: /usr/lib/systemd/system/ssh.service.d
└─ec2-instance-connect.conf
Active: active (running) since Wed 2024-09-04 09:08:36 UTC; 1min 5s ago
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 1017 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 1019 (sshd)
Tasks: 1 (limit: 1078)
Memory: 3.9M (peak: 4.4M)
CPU: 52ms
CGroup: /system.slice/ssh.service
└─1019 "sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorize
Sep 04 09:08:36 ip-172-31-47-12 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 04 09:08:36 ip-172-31-47-12 sshd[1019]: Server listening on :: port 22.
Sep 04 09:08:36 ip-172-31-47-12 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Sep 04 09:08:39 ip-172-31-47-12 sshd[1020]: Accepted publickey for ubuntu from 103.135.95.46 port 51936 ssh2: RSA SHA25
Sep 04 09:08:39 ip-172-31-47-12 sshd[1020]: pam_unix(sshd:session): session o
pened for user ubuntu(uid=1000) by ubuntu(
ubuntu@ip-172-31-47-12:~$
Type here to search
28°C Partly sunny
ENG
14:39
04-09-2024


ubuntu@ip-172-31-47-12: ~
ubuntu@ip-172-31-47-12:~$ sudo passwd ubuntu
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-47-12:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
Drop-In: /usr/lib/systemd/system/ssh.service.d
└─ec2-instance-connect.conf
Active: active (running) since Wed 2024-09-04
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 1017 ExecStartPre=/usr/sbin/sshd -t (c
Main PID: 1019 (sshd)
Tasks: 1 (limit: 1078)
Memory: 3.9M (peak: 4.4M)
CPU: 52ms
CGroup: /system.slice/ssh.service
└─1019 "sshd: /usr/sbin/sshd -D -o AutI
Sep 04 09:08:36 ip-172-31-47-12 systemd[1]: Startin
Sep 04 09:08:36 ip-172-31-47-12 sshd[1019]: Server
Sep 04 09:08:36 ip-172-31-47-12 systemd[1]: Started
Sep 04 09:08:39 ip-172-31-47-12 sshd[1020]: Accepte
pened for user ubuntu(uid=1000) by ubuntu(
ubuntu@ip-172-31-47-12:~$ sudo vim /etc/ssh/sshd_c
ubuntu@ip-172-31-47-12:~$ sudo vim /etc/ssh/sshd_c
ubuntu@ip-172-31-47-12:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.se
Drop-In: /usr/lib/systemd/system/ssh.service.d
└─ec2-instance-connect.conf
Active: active (running) since Wed 2024-09-04
TriggeredBy: ● ssh.socket
Docs: man:sshd(8)
man:sshd_config(5)
Process: 1017 ExecStartPre=/usr/sbin/sshd -t (c
Main PID: 1019 (sshd)
Tasks: 1 (limit: 1078)
Memory: 3.9M (peak: 4.4M)
CPU: 52ms
CGroup: /system.slice/ssh.service
└─1019 "sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %u %f -o AuthorizedKeysCommandUser ec2-instance-connect [listener] 0 c
Sep 04 09:08:36 ip-172-31-47-12 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 04 09:08:36 ip-172-31-47-12 sshd[1019]: Server listening on :: port 22.
Sep 04 09:08:36 ip-172-31-47-12 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Sep 04 09:08:39 ip-172-31-47-12 sshd[1020]: Accepted publickey for ubuntu from 103.135.95.46 port 51936 ssh2: RSA SHA256:8uN4RP4MSbhYeFfxxWAmdy9MPC34hnsE7cx7+GCDkr4
Sep 04 09:08:39 ip-172-31-47-12 sshd[1020]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
ubuntu@ip-172-31-47-12:~$ touch text.txt
ubuntu@ip-172-31-47-12:~$
ubuntu@ip-172-31-47-37: ~
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-47-37:~$ ssh_keygen
Command 'ssh_keygen' not found, did you mean:
command 'ssh-keygen' from deb openssh-client (1:9.6p1-3ubuntu13.4)
Try: sudo apt install <deb name>
ubuntu@ip-172-31-47-37:~$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/ubuntu/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ubuntu/.ssh/id_ed25519
Your public key has been saved in /home/ubuntu/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:4Qc3W8OhNd+RhPOBGSlGgWdK7+qgTsxun14P6FNlcRg ubuntu@ip-172-31-47-37
The key's randomart image is:
+--[ED25519 256]--+
| E=o=.Bo.|
| = X X +.|
| + % = + o|
| . B = . . |
| S + |
| o .. . . |
| =.+ . |
| +o+ +. |
| =O. .o |
+----[SHA256]-----+
ubuntu@ip-172-31-47-37:~$
ubuntu@ip-172-31-47-37:~$ ssh-copy-id ubuntu
sshd:session): session o
Type here to search
28°C Partly sunny
ENG
15:05
04-09-2024





All the commands have been executed and the output has been obtained successfully.